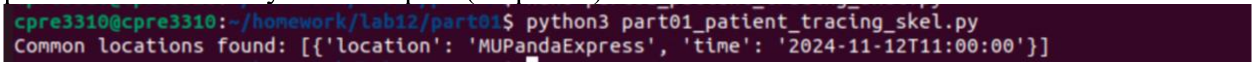
Lab 12 Template – Ethan Roepke

Some questions require multiple parts to be answered, be sure to discuss them in full.

Part 01:

1. Take a screenshot of the location and time where you were in contact with the COVID-19 patient to include in your lab report (10 points)



```
cpre3310@cpre3310:~/homework/lab12/part01$ python3 part01_patient_tracing_skel.py
Common locations found: [{'location': 'MUPandaExpress', 'time': '2024-11-12T11:00:00'}]
```

2. Upload your code to Canvas (10 points)

   UPLOADED

3. Please provide another real-world example where PSI could be beneficial. Justify your reasons why it maintains confidentiality and privacy in your proposed use case. Explain how it benefits public good and protects individual rights (25 total points)

   Another real-world example where PSI could be beneficial is in the banking business. Specifically to battle against fraudulent activity. If banks suspect that accounts are participating in fraudulent activities from scams or laundering money. Banks will not share account information to other banks for privacy and competitive concerns, but they can use PSI to securely compare customers accounts to identify if have matching or similar accounts without revealing any account information. Using PSI maintains confidentiality and privacy by not displaying any personal bank accounts and only displaying matching accounts to detect for fraud between both banks without compromising data privacy.

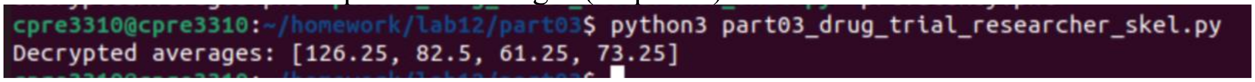
Part 02:

4. Upload your code to Canvas (10 points)

   UPLOADED

Part 03:

5. Take a screenshot of the 4 plaintext averages (10 points)



```
cpre3310@cpre3310:~/homework/lab12/part03$ python3 part03_drug_trial_researcher_skel.py
Decrypted averages: [126.25, 82.5, 61.25, 73.25]
```

6. Upload your code to Canvas (10 points)

   UPLOADED

7. How could partially homomorphic encryption be effectively used in an election? 3 viewpoints (25 total points, 8.33 points each perspective)

   Poll workers perspective:

   PHE can ensure secure and efficient handling of votes. When voters cast their vote on a tablet, PHE will encrypt the votes before leaving for counting. The votes being encrypted does not allow the poll workers to be able to modify or see the votes. This gives trust for voters knowing their vote cannot be modified. The poll workers can focus more on verifying the voters identity and other duties for smooth voting days.

Vote counters perspective:
PHE will give accurate and efficient tallying when it comes to the vote counters. When the workers tally, the ballots will not need to be decrypted and PHE can do mathematical operations directly on the encrypted ballots. This means that the votes will maintain voters confidentiality and produce a verified tally of ballots.

Election officials perspective:
At this step, PHE will simplify the process of compiling and reporting the results for all to view. The ballots still remain encrypted so they are still unable to view voters personal information or change the vote. For the election officials, they can maintain confidence in the electoral system while fulfilling their duty to deliver the results in timely manner and accurate tallies.